(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001243062 A**

(43) Date of publication of application: **07.09.01**

(51) Int. Cl **G06F 9/06**
G06F 9/445

(21) Application number: **2000056472**

(22) Date of filing: **01.03.00**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

(72) Inventor: **MORIMURA KAZUO**
ITO SHUICHI
ADACHI YOSHIHIKO
NIWANO EIICHI

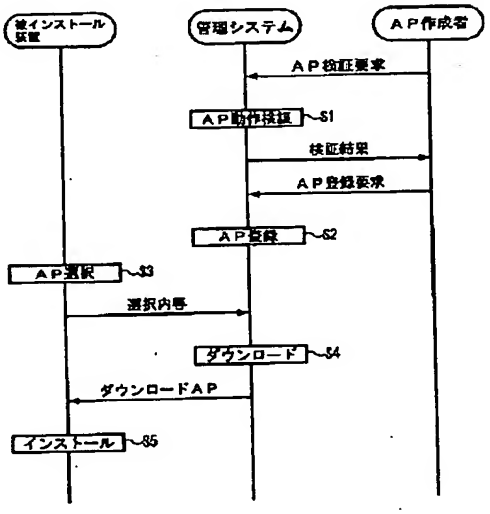
(54) METHOD AND SYSTEM FOR MANAGING APPLICATION PROGRAM AND STORAGE MEDIUM WITH APPLICATION PROGRAM MANAGEMENT PROGRAM STORED THEREIN

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an AP managing method and system capable of guaranteeing the operation of an AP and a storage medium with an AP management program stored therein.

SOLUTION: This system is provided with an AP verifying mechanism for verifying the operation of a prepared application and an AP managing mechanism for managing the verified AP independently of each other. The operation of the AP prepared by an AP preparer is verified by the AP verifying mechanism, and when it is correct, a warranty is issued, and returned to the AP preparer, and the unitary management of the AP whose warranty is issued is operated by the AP managing mechanism. When the desired AP is selected from an installed device, and when a request for down-load is issued, the AP corresponding to the request is down-loaded together with the warranty applied to the AP from among the AP under the unitary management. The installed device verifies the down-loaded AP based on the warranty applied to the AP, and when the verification is correct, installs the AP inside its own device.

本発明の原理を説明するための図



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－243062
（P2001－243062A）
(43)公開日　平成13年９月７日(2001.9.7)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｚ　５Ｂ０７６
9/445			４２０Ｊ

審査請求　未請求　請求項の数15　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－56472(P2000－56472)

(22)出願日　平成12年３月１日(2000.3.1)

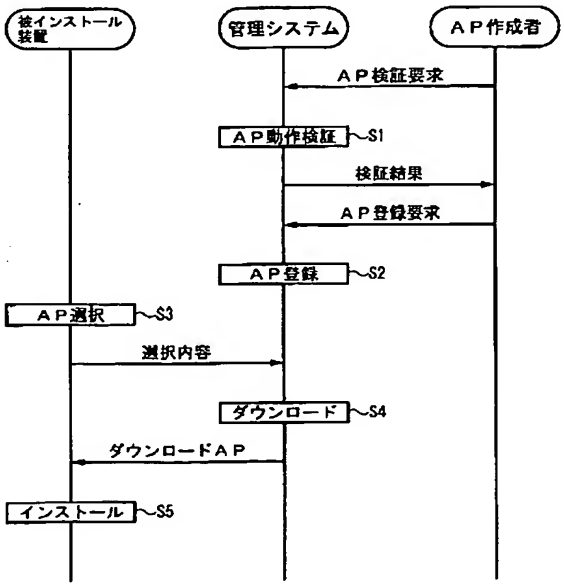
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　森村　一雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　伊藤　修一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　アプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体

(57)【要約】
【課題】　ＡＰの動作を保証することが可能なＡＰ管理方法及びシステム及びＡＰ管理プログラムを格納した記憶媒体を提供する。
【解決手段】　本発明は、作成されたアプリケーションの動作を検証するためのＡＰ検証機構と、検証されたＡＰを管理するＡＰ管理機構とを独立して設け、ＡＰ検証機構において、ＡＰ作成者が作成したＡＰの動作を検証し、正しければ、保証書を発行し、該ＡＰ作成者に返却し、保証書が発行されたＡＰをＡＰ管理機構で一元管理し、被インストール装置から所望のＡＰが選択され、ダウンロードの要求が発行された際に、一元管理されているＡＰの中から要求に対応するＡＰを、該ＡＰに付与されている保証書と共にダウンロードし、被インストール装置では、ダウンロードされたＡＰを該ＡＰに付与されている保証書に基づいて検証し、検証が正しければ該ＡＰを自装置内にインストールする。

本発明の原理を説明するための図



1

【特許請求の範囲】

【請求項１】　作成されたアプリケーションプログラムを管理するためのアプリケーション管理方法において、作成されたアプリケーションの動作を検証するためのアプリケーションプログラム検証機構と、検証されたアプリケーションプログラムを管理するアプリケーションプログラム管理機構とを独立して設け、

前記アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証し、正しければ、保証書を発行し、該アプリケーションプログラム作成者に返却し、

前記保証書が発行されたアプリケーションプログラムを前記アプリケーションプログラム管理機構で一元管理し、

被インストール装置から所望のアプリケーションプログラムが選択され、ダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードし、

前記被インストール装置では、前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている前記保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールすることを特徴とするアプリケーションプログラム管理方法。

【請求項２】　前記アプリケーションプログラム検証機構において、前記アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与された前記アプリケーションプログラムを受け取り、

前記アプリケーションプログラムを検証し、検証結果が正しければ、前記アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて前記保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する請求項１記載のアプリケーションプログラム管理方法。

【請求項３】　前記アプリケーションプログラム管理機構において、前記アプリケーションプログラム作成者から、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書を受け取ると、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書の組に対して秘密鍵を用いて署名し、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書及び前記アプリケーションプログラム管理機構の署名の組をデータベースに格納する請求項１記載のアプリケーションプログラム管理方法。

2

【請求項４】　前記被インストール装置において、

前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証し、

検証結果が正しい場合には、前記保証書に格納された前記アプリケーションプログラム検証機構の署名を、前記アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、前記アプリケーションプログラムを記憶手段にインストールする請求項１記載のアプリケーションプログラム管理方法。

【請求項５】　前記アプリケーションプログラムは、

ＩＣカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする請求項１乃至４記載のアプリケーションプログラム管理方法。

【請求項６】　前記被インストール装置は、

ＩＣカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする請求項１乃至４記載のアプリケーションプログラム管理方法。

【請求項７】　作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムであって、

前記アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証手段と、前記検証手段による検証が正しければ、保証書を発行する保証書発行手段と、該アプリケーションプログラム作成者に返却する返却手段とを有するアプリケーションプログラム検証機構と、

前記保証書が発行されたアプリケーションプログラムを前記アプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持手段と、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供手段とを有するアプリケーションプログラム管理機構とを有する管理システムと、

前記アプリケーションプログラム管理機構に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択手段と、

前記アプリケーションプログラム管理機構からアプリケーションプログラムをダウンロードされるダウンロード手段と、

前記ダウンロード手段によりダウンロードされたアプリ

ケーションプログラムを該アプリケーションプログラムに付与されている前記保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストール手段とを有する被インストール装置とを有することを特徴とするアプリケーションプログラム管理システム。

【請求項８】　前記アプリケーションプログラム検証機構の前記検証手段は、

前記アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与された前記アプリケーションプログラムを受け取る手段と、

前記アプリケーションプログラムを検証し、検証結果が正しければ、前記アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて前記保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する手段を含み、

前記アプリケーションプログラム管理機構は、

前記アプリケーションプログラム作成者から、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書を受け取る手段と、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書の組に対して秘密鍵を用いて署名する手段と、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書及び前記アプリケーションプログラム管理機構の署名の組をデータベースに格納する手段を含む請求項７記載のアプリケーションプログラム管理システム。

【請求項９】　前記被インストール装置の前記インストール手段は、

前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証する手段と、

検証結果が正しい場合には、前記保証書に格納された前記アプリケーションプログラム検証機構の署名を、前記アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、前記アプリケーションプログラムを記憶手段にインストールする手段を含む請求項７記載のアプリケーションプログラム管理システム。

【請求項１０】　前記アプリケーションプログラムは、ＩＣカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする請求項７乃至９記載のアプリケーションプログラム管理システム。

【請求項１１】　前記被インストール装置は、ＩＣカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする請求項７乃至９記載のアプリケーションプログラム管理システム。

【請求項１２】　作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、該アプリケーションプログラムを一元管理する管理システムに搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、

前記アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証プロセスと、前記検証プロセスによる検証が正しければ、保証書を発行する保証書発行プロセスと、該アプリケーションプログラム作成者に返却する返却プロセスとを有するアプリケーションプログラム検証プログラムモジュールと、

前記保証書が発行されたアプリケーションプログラムを前記アプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持プロセスと、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供プロセスとを有するアプリケーションプログラム管理プログラムモジュールとを有することを特徴とするアプリケーションプログラム管理プログラムを格納した記憶媒体。

【請求項１３】　前記アプリケーションプログラム検証プログラムモジュールの前記検証プロセスは、

前記アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与された前記アプリケーションプログラムを受け取るプロセスと、

前記アプリケーションプログラムを検証し、検証結果が正しければ、前記アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて前記保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却するプロセスを含み、

前記アプリケーションプログラム管理プログラムモジュールは、

前記アプリケーションプログラム作成者から、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書を受け取るプロセスと、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書の組に対して秘密鍵を用いて署名するプロセスと、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書及び前記アプリケーションプログラム管理機構の署名の組をデータベースに格納するプロセスを含む請求項１２記載のアプリ

ケーションプログラム管理プログラムを格納した記憶媒体。

【請求項１４】　作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、独立して設けられている、アプリケーションプログラムを検証するためのアプリケーションプログラム検証機構とアプリケーションプログラムを一元管理するアプリケーションプログラム管理機構からなる管理システムからアプリケーションプログラムを取得する被インストール装置に搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、

前記アプリケーションプログラム管理機構に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択プロセスと、

前記アプリケーションプログラム管理機構からアプリケーションプログラムをダウンロードされるダウンロードプロセスと、

前記ダウンロードプロセスによりダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている前記保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストールプロセスとを有することを特徴とするアプリケーションプログラム管理プログラムを格納した記憶媒体。

【請求項１５】　前記インストールプロセスは、

前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証するプロセスと、

検証結果が正しい場合には、前記保証書に格納された前記アプリケーションプログラム検証機構の署名を、前記アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、前記アプリケーションプログラムを記憶手段にインストールするプロセスを含む請求項１４記載のアプリケーションプログラム管理プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、アプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体に係り、特に、アプリケーションプログラム検証機構にて動作検証がなされたアプリケーションプログラムを、アプリケーション管理機構にて一元管理するためのアプリケーションプログラムを管理するシステムにおいて、末端利用者端末用アプリケーションプログラム等をネットワーク経由でダウンロードして、ＩＣカードや利用者保有の端末にインストールし、ＩＣカード用アプリケーションプログラム及び利用者端末用アプリケーションプログラムの普及及び流通を促進するためのアプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体に関する。

【０００２】

【従来の技術】従来においては、アプリケーションプログラムの動作検証を行うアプリケーションプログラム検証機構、及びアプリケーションプログラムの一元管理を行うアプリケーションプログラム管理機構は存在しないので、アプリケーションプログラム、及びＩＣカード用アプリケーションプログラム、及び、利用者端末用アプリケーションプログラムの動作保証は、アプリケーションプログラムを利用する末端利用者が自らの責任で実施する必要がある。

【０００３】図７は、従来のアプリケーションプログラム管理方法の動作のフローチャートである。

【０００４】ステップ１０）　選択処理過程において、末端利用者は、アプリケーションプログラムを利用者端末または、ＩＣカードにインストールする際に、各アプリケーション作成者１０４、１０５、１０６、１０７に接続して所望のアプリケーションプログラムを選択する。

【０００５】ステップ１１）　ダウンロード処理過程において、各アプリケーション作成者１０４、１０５、１０６、１０７から所望のアプリケーションプログラムをダウンロードする。

【０００６】ステップ１２）　インストール処理過程において、利用者端末または、ＩＣカードにインストールする。

【０００７】

【発明が解決しようとする課題】しかしながら、上記従来の方法では、例えば、前述の図７の場合、末端利用者が利用者端末または、ＩＣカードに新たなアプリケーションプログラムをインストールしようとする場合、各アプリケーション作成者が正当な存在であるか、または、各アプリケーション作成者が管理しているアプリケーションプログラムが正当なものであるかは一般には分からない。

【０００８】従って、各アプリケーション作成者からアプリケーションプログラムをダウンロードしてインストールする際は、その動作保証は、アプリケーションプログラムを利用する末端利用者から自らの責任で実施する必要がある。

【０００９】本発明は、上記の点に鑑みなされたもので、アプリケーションプログラムの動作を保証することが可能なアプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。

【００１１】本発明（請求項１）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理方法において、作成されたアプリケーションの動作を検証するためのアプリケーションプログラム検証機構と、検証されたアプリケーションプログラムを管理するアプリケーションプログラム管理機構とを独立して設け、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証し（ステップ１）、正しければ、保証書を発行し、該アプリケーションプログラム作成者に返却し、保証書が発行されたアプリケーションプログラムをアプリケーションプログラム管理機構で一元管理し（ステップ２）、被インストール装置において、所望のアプリケーションプログラムが選択され、ダウンロードの要求が発行された際に（ステップ３）、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードし（ステップ４）、被インストール装置では、アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールする（ステップ５）。

【００１２】本発明（請求項２）は、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与されたアプリケーションプログラムを受け取り、アプリケーションプログラムを検証し、検証結果が正しければ、アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する。

【００１３】本発明（請求項３）は、アプリケーションプログラム管理機構において、アプリケーションプログラム作成者から、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書を受け取ると、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書の組に対して秘密鍵を用いて署名し、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書及びアプリケーションプログラム管理機構の署名の組をデータベースに格納する。

【００１４】本発明（請求項４）は、被インストール装置において、アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証し、検証結果が正しい場合には、保証書に格納されたアプリケーションプログラム検証機構の署名を、アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、アプリケーションプログラムを記憶手段にインストールする。

【００１５】本発明（請求項５）は、アプリケーションプログラムとして、ＩＣカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする。

【００１６】本発明（請求項６）は、被インストール装置として、ＩＣカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする。

【００１７】図２は、本発明の原理構成図である。

【００１８】本発明（請求項７）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムであって、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証手段と、検証手段による検証が正しければ、保証書を発行する保証書発行手段と、該アプリケーションプログラム作成者に返却する返却手段とを有するアプリケーションプログラム検証機構１１０と、保証書が発行されたアプリケーションプログラムをアプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持手段と、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供手段とを有するアプリケーションプログラム管理機構１２０とを有する管理システム１００と、アプリケーションプログラム管理機構１２０に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択手段３１０と、アプリケーションプログラム管理機構１２０からアプリケーションプログラムをダウンロードされるダウンロード手段３２０と、ダウンロード手段３２０によりダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストール手段３３０とを有する。

【００１９】本発明（請求項８）は、アプリケーションプログラム検証機構１１０の検証手段において、アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与されたアプリケーションプログラムを受け取る手段と、アプリケーションプログラムを検証し、検証結果が正しければ、アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて保証書を生成し、

該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する手段を含み、アプリケーションプログラム管理機構１２０において、アプリケーションプログラム作成者から、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書を受け取る手段と、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書の組に対して秘密鍵を用いて署名する手段と、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書及びアプリケーションプログラム管理機構の署名の組をデータベースに格納する手段を含む。

【００２０】本発明（請求項９）は、被インストール装置３００のインストール手段３３０は、アプリケーションプログラム管理機構１２０からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構１２０の署名を、該アプリケーションプログラム管理機構１２０の公開鍵を用いて検証する手段と、検証結果が正しい場合には、保証書に格納されたアプリケーションプログラム検証機構１１０の署名を、アプリケーションプログラム管理機構１２０の署名を用いて検証し、検証結果が正しければ、アプリケーションプログラムを記憶手段にインストールする手段を含む。

【００２１】本発明（請求項１０）は、アプリケーションプログラムとして、ＩＣカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする。

【００２２】本発明（請求項１１）は、被インストール装置として、ＩＣカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする。

【００２３】本発明（請求項１２）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、該アプリケーションプログラムを一元管理する管理システムに搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証プロセスと、検証プロセスによる検証が正しければ、保証書を発行する保証書発行プロセスと、該アプリケーションプログラム作成者に返却する返却プロセスとを有するアプリケーションプログラム検証プログラムモジュールと、保証書が発行されたアプリケーションプログラムをアプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持プロセスと、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供プロセスとを有するアプリケーションプログラム管理プログラムモジュールとを有する。

【００２４】本発明（請求項１３）は、アプリケーションプログラム検証プログラムモジュールの検証プロセスにおいて、アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与されたアプリケーションプログラムを受け取るプロセスと、アプリケーションプログラムを検証し、検証結果が正しければ、アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却するプロセスを含み、アプリケーションプログラム管理プログラムモジュールにおいて、アプリケーションプログラム作成者から、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書を受け取るプロセスと、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書の組に対して秘密鍵を用いて署名するプロセスと、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書及びアプリケーションプログラム管理機構の署名の組をデータベースに格納するプロセスを含む。

【００２５】本発明（請求項１４）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、独立して設けられている、アプリケーションプログラムを検証するためのアプリケーションプログラム検証機構とアプリケーションプログラムを一元管理するアプリケーションプログラム管理機構からなる管理システムからアプリケーションプログラムを取得する被インストール装置に搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、アプリケーションプログラム管理機構に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択プロセスと、アプリケーションプログラム管理機構からアプリケーションプログラムをダウンロードされるダウンロードプロセスと、ダウンロードプロセスによりダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストールプロセスとを有する。

【００２６】本発明（請求項１５）は、インストールプロセスにおいて、アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証するプロセスと、検証結果が正しい場合には、保証書に格納されたアプリケーションプログラム検証機構の署

名を、アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、アプリケーションプログラムを記憶手段にインストールするプロセスを含む。

【００２７】上記のように、本発明では、アプリケーションプログラムの動作を保証するためのアプリケーションプログラム検証機構と、動作保証されたアプリケーションプログラムを管理するためのアプリケーションプログラム管理機構を導入することにより、アプリケーションプログラム管理機構に蓄えられるアプリケーションプログラムは、その動作及び製造元を保証されているので、末端利用者が自ら動作検証等を行う必要がなくなる。

【００２８】

【発明の実施の形態】以下の説明において、アプリケーションプログラム（以下、ＡＰと記す）は、ＩＣ／カード用ＡＰ、利用者端末用ＡＰ、ホスト用ＡＰ、サーバ用ＡＰ、クライアント用ＡＰ等のプログラムを抽象化した用語である。

【００２９】図３は、本発明のＡＰ管理システムの構成を示す。

【００３０】同図に示すシステムは、管理装置１００、ＡＰ作成者装置２００、利用者装置３００から構成される。

【００３１】管理装置１００は、ＡＰ作成者装置２００、利用者装置３００とは独立に設けられた装置であり、ＡＰ検証機構１１０とＡＰ管理機構１２０から構成される。これらの構成については、後述する。

【００３２】ＡＰ作成装置２００は、管理装置のＡＰ検証機構１１０にＡＰの検証を依頼する検証依頼部２１０と、検証され、検証結果として、その正当性が保証されたプログラムの登録をＡＰ管理機構１２０に対して依頼する登録部２２０から構成される。当該ＡＰ作成者装置２００は、ＡＰ作成者毎に有するものとし、同図では、説明の簡単化のため、１つのＡＰ作成者装置２００のみを示しているが実際には、複数台が存在するものとする。

【００３３】利用者装置３００は、管理装置１００のＡＰ管理機構１２０にダウンロードしたいＡＰを選択して通知する選択部３１０と、ＡＰ管理機構１２０から、選択部３１０で選択したＡＰがダウンロードされるダウンロード部３２０、ダウンロード部３２０においてダウンロードされたＡＰをインストールするインストール部３３０から構成される。また、同図では、説明の簡単化のため、１つの利用者装置３００のみを示してるが、利用者毎に有するものとし、実際には複数台が存在するものとする。

【００３４】次に、管理装置１００のＡＰ検証機構１１０の構成について説明する。

【００３５】図４は、本発明のＡＰ検証機構の構成を示す。

【００３６】ＡＰ検証機構１１０は、ＡＰ・署名受取部り部１１１、動作検証部１１２、保証書発行部１１３、及びＡＰ・署名・保証書返却部１１４から構成される。

【００３７】次に、ＡＰ検証機構１１０におけるＡＰの検証動作について説明する。

【００３８】以下の説明において、ＡＰ検証機構１１０の保証書発行部１１３は、保証書を発行するための秘密鍵１１５を有し、ＡＰ作成者装置２００についてもそれぞれ秘密鍵３１０～３１３を有するものとする。

【００３９】ＡＰ・署名受取部１１１は、作成者装置２００の検証依頼部２１０からの検証依頼情報（ＡＰ、作成者署名）を受け取る。

【００４０】動作検証部１１２は、ＡＰ・署名受取部１１１で取得したＡＰについて動作を検証する。

【００４１】保証書発行部１１３は、動作検証部１１２において検証された動作に問題がなければ、保証書を発行する。このとき、保証書は、ＡＰ及びＡＰ作成者署名に対して、ＡＰ検証機構１１０が固有に保持する秘密鍵１１５を用いて付与する署名・動作環境・動作保証期間等のデータが含まれるものとする。

【００４２】ＡＰ・署名・保証書返却部１１４は、ＡＰ、署名及び、保証書発行部１１３で発行された保証書をＡＰ作成者装置２００に返却する。

【００４３】次に、管理装置１００のＡＰ管理機構１２０の構成について説明する。

【００４４】図５は、本発明のＡＰ管理機構の構成を示す。

【００４５】同図に示すＡＰ管理機構１２０は、ＡＰ・署名・保証書受取部１２１、署名付与部１２２、ＤＢ格納部１２３、ＡＰＤＢ１２４から構成される。

【００４６】ＡＰ・署名・保証書受取部１２１は、ＡＰ作成者装置２００の登録部２２０から送られてくるＡＰ、作成者署名、保証書を受け取る。

【００４７】署名付与部１２２は、ＡＰ・署名・保証書受取部１２１で受け取ったＡＰとＡＰ作成者署名と保証書に対して、ＡＰ管理機構１２０で有する秘密鍵１２５を用いて署名する。

【００４８】ＤＢ格納部１２３は、ＡＰ及びＡＰ作成者署名及び保証書及びＡＰ管理機構署名をアプリケーション管理ＤＢ１２３に格納する。

【００４９】次に、上記の構成における動作を説明する。

【００５０】ステップ１０１）　ＡＰ作成者装置２００の検証依頼部２１０からＡＰと署名を検証依頼情報として管理装置１００のＡＰ検証機構１１０に送る。

【００５１】ステップ１０２）　管理装置１００のＡＰ検証機構１１０の動作検証部１１２では、取得した検証依頼情報に基づいて、ＡＰを検証する。

【００５２】ステップ１０３）　動作検証部１１２にお

いて、検証結果が正しければ、秘密鍵１１５を用いて保証書を発行する。

【００５３】ステップ１０４）　ＡＰ・署名・保証書返却部１１４は、検証したＡＰ、署名・保証書をＡＰ作成者装置２００に返却する。

【００５４】ステップ１０５）　ＡＰ作成者装置２００の登録部２２０において、管理装置１００のＡＰ管理機構１２０に対して、ＡＰ、署名、及び保証書を管理依頼情報として送る。

【００５５】ステップ１０６）　ＡＰ管理機構１２０の署名付与部１２２では、当該情報に対して秘密鍵１２５を用いてＡＰ管理機構署名を付与する。

【００５６】ステップ１０７）　ステップ１２１で受け取ったＡＰ、作成者署名、保証書、及びステップ１０６で生成されたＡＰ管理機構署名をアプリケーション管理ＤＢ１２４に格納する。

【００５７】ステップ１０８）　次に、利用者装置３００の選択部３１０からＡＰの選択要求が発行される。

【００５８】ステップ１０９）　管理装置１００のＡＰ管理機構１２０は、利用者装置３００からの要求に基づいて、選択されたＡＰをアプリケーション管理ＤＢ１２４から検索し、ＡＰ，ＡＰ作成者署名、保証書、及びＡＰ管理機構署名を利用者装置３００のダウンロード部３２０にダウンロードする。

【００５９】ステップ１１０）　利用者装置３００のインストール部３３０は、ダウンロードされたＡＰを装置内の記憶手段にインストールする。このときの処理は、以下の通りである。

【００６０】・　ダウンロードされたＡＰ管理機構署名を、ＡＰ管理機構１２０の公開鍵を用いて検証する。

【００６１】・　保証書に格納されたＡＰ検証機構１１０の署名の検証結果が正しかった場合には、ダウンロードされたＡＰ作成者署名を、ＡＰ作成者の公開鍵を用いて検証する。

【００６２】・　ＡＰ作成者署名の検証結果が正しかった場合には、ダウンロードされたＡＰを、利用者端末３００内の二次記憶装置内、あるいは、ＩＣカード内にインストールする。

【００６３】

【実施例】以下、図面と共に本発明の実施例を説明する。

【００６４】まず、実施例では、種々のＡＰの種類に応じたインストールについて説明する。

【００６５】（１）ＡＰの種類がＩＣカード用ＡＰである場合：前述のステップ１１０において、インストールされるＡＰがＩＣカード用ＡＰの場合には、インストールされる記憶媒体は、ＩＣカード内となる。

【００６６】（２）ＡＰの種類が利用者端末用のＡＰである場合：前述のステップ１１０において、インストールされるＡＰが利用者端末用ＡＰの場合には、インストールされる記憶媒体は、利用者端末の二次記憶装置内となる。

【００６７】（３）ＡＰの種類がホスト用ＡＰである場合：前述のステップ１１０において、インストールされるＡＰがホスト用ＡＰの場合には、インストールされる記憶媒体は、ホストの二次記憶装置内となる。

【００６８】（４）ＡＰの種類がサーバ用ＡＰである場合：前述のステップ１１０において、インストールされるＡＰがホスト用ＡＰの場合には、インストールされる記憶媒体は、サーバの二次記憶装置内となる。

【００６９】（５）ＡＰの種類がクライアント用ＡＰである場合：前述のステップ１１０において、インストールされるＡＰがクライアント用ＡＰの場合には、インストールされる記憶媒体は、クライアントの二次記憶装置内となる。

【００７０】また、図３の構成において、利用者端末３００と管理装置１００とをネットワークを介して接続し、当該ネットワークを介して管理装置１００からダウンロードされたＡＰをインストールすることも可能である。

【００７１】また、図３の利用者端末３００の代わりに、ＩＣカード端末をネットワークを介して管理装置１００と接続し、当該ネットワークを介して管理装置１００からダウンロードされたＩＣカード用ＡＰをインストールすることも可能である。

【００７２】また、図３の利用者端末３００の代わりに、ホストをネットワークを介して管理装置１００と接続し、当該ネットワークを介して管理装置１００からダウンロードされたホスト用ＡＰをインストールすることも可能である。

【００７３】また、図３の利用者端末３００の代わりに、サーバをネットワークを介して管理装置１００と接続し、当該ネットワークを介して管理装置１００からダウンロードされたサーバ用ＡＰをインストールすることも可能である。

【００７４】さらに、図３の利用者端末３００の代わりに、クライアントをネットワークを介して管理装置１００と接続し、当該ネットワークを介して管理装置１００からダウンロードされたクライアント用ＡＰをインストールすることも可能である。また、図３に示す管理装置１００のＡＰ検証機構１１０については、図４に示す各構成要素を、ＡＰ管理機構１２０については、図５に示す各構成要素をプログラムとして構築し、管理装置１００として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【００７５】また、本発明は、記憶媒体を読み取るための読み取り装置と、記憶媒体から読み取ったプログラムや各ＡＰファイルを格納し、それを自由に読み出し可能

なメモリ装置と、各種の操作を行う際に必要なデータを保持するためのバッファやそれに準ずる装置と、その処理の過程で必要な情報等を表示するためのディスプレイ等の出力装置と、ＡＰの検索条件等の必要な指示を与えるためのキーボードやマウス等の入力装置とを備え、それらのメモリ装置、バッファ、出力装置及び入力装置等を上記プログラムによって予め定められた手順に基づいて、制御するコンピュータや、それに準ずる装置により、図３～図６に示した各構成要素、各処理の手順乃至、アルゴリズムを適宜実行することが可能である。また、その手順乃至アルゴリズムをコンピュータ等に実行させるためのプログラムを上記の読み取り装置が読み取り可能な記憶媒体、例えば、フロッピー（登録商標）ディスクやメモリカード、ＭＯ，ＣＤ，ＤＶＤ等に記録して配布することが可能である。

【００７６】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【００７７】

【発明の効果】上述のように、本発明によれば、末端利用者にとっては、ＡＰの動作検証作業から開放される。また、ＡＰの開発者にとっては、末端利用者へＡＰが配布されるまでの間に、ＡＰが不正に改ざんされる危険性がなくなり、開発したＡＰの普及が促進される。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明のアプリケーションプログラム管理システムの構成図である。

【図４】本発明のアプリケーションプログラム検証機構＊の構成図である。

【図５】本発明のアプリケーションプログラム管理機構の構成図である。

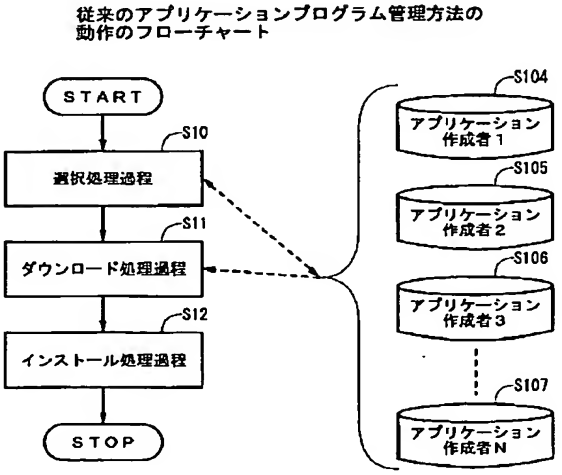
【図６】本発明のアプリケーションプログラム管理処理のシーケンスチャートである。

【図７】従来のアプリケーションプログラム管理方法の動作のフローチャートである。

【符号の説明】

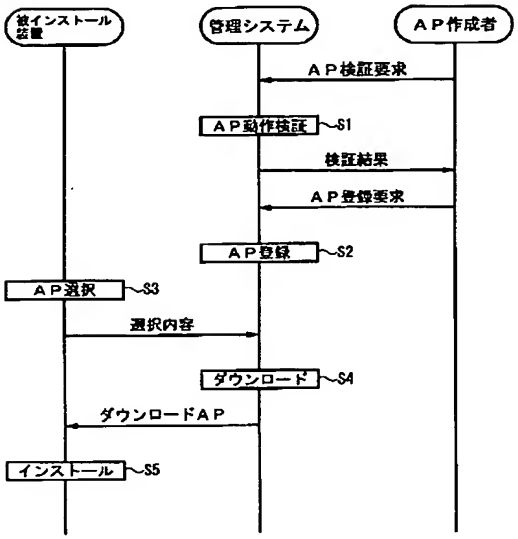
１００　管理システム、管理装置
１１０　アプリケーションプログラム検証機構
１１１　アプリケーションプログラム・署名・受取部
１１２　動作検証部
１１３　保証書発行部
１１４　アプリケーションプログラム・署名・保証書返却部
１１５　秘密鍵
１２０　アプリケーションプログラム管理機構
１２１　アプリケーションプログラム・署名・保証書受取部
１２２　署名付与部
１２３　ＤＢ格納部
１２４　アプリケーション管理ＤＢ
１２５　秘密鍵
２００　作成者装置
２１０　検証要求手段、検証依頼部
２２０　登録要求手段、登録部
３００　被インストール装置、利用者装置
３１０　アプリケーションプログラム選択手段、選択部
３２０　ダウンロード手段、ダウンロード部
３３０　インストール手段、インストール部

【図７】



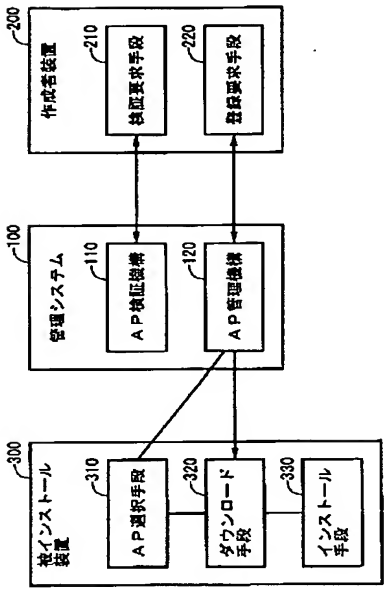
【図１】

本発明の原理を説明するための図



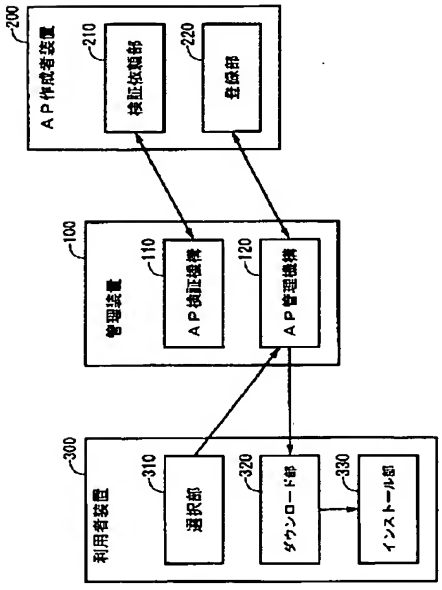
【図２】

本発明の原理構成図



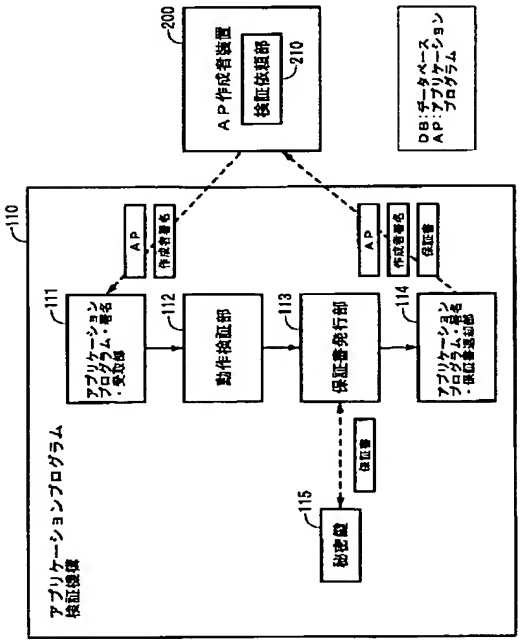
【図３】

本発明のＡＰ管理システム構成図



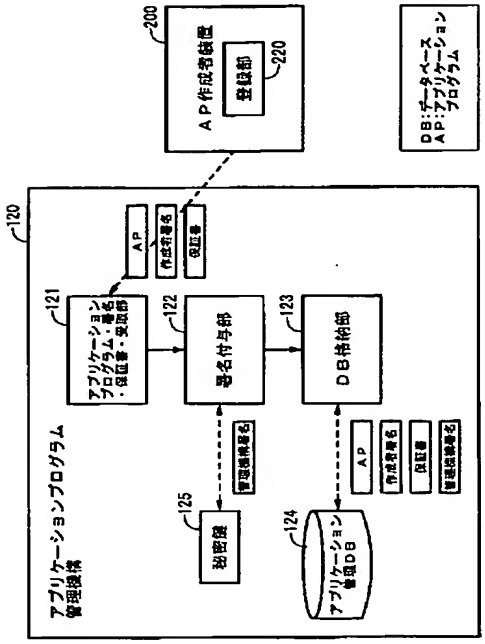
【図４】

本発明のアプリケーションプログラム検証機構の構成図



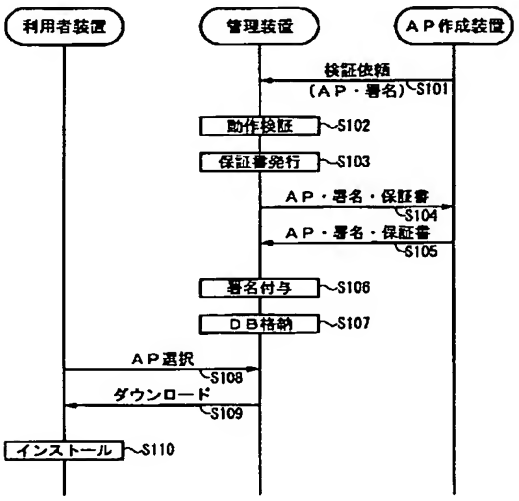
【図５】

本発明のアプリケーション管理機構の構成図



【図６】

本発明のアプリケーション管理処理のシーケンスチャート



フロントページの続き

(72)発明者　足立　佳彦
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者　庭野　栄一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B076 AB10 BB06 FA13